

AFFIDAVIT OF VIVIAN M. BARRIOS IN SUPPORT OF CRIMINAL COMPLAINT

I, Special Agent Vivian M. Barrios, being duly sworn state:

INTRODUCTION

1. I have been a Special Agent for the Federal Bureau of Investigation (“FBI”) since 2014 and am currently assigned to the Economic Crimes squad in Boston, Massachusetts. I received my Bachelor of Arts from the University of Colorado in 2002 and my Juris Doctorate from the University of Denver in 2005. In my current position as a Special Agent, I investigate white-collar crime, including money laundering, mail fraud, wire fraud, and bank fraud, among other things. I also have experience investigating telemarketing fraud, and through that work, have gained familiarity with computer and smartphone-based communication applications such as WhatsApp and Skype.

PROBABLE CAUSE TO BELIEVE FEDERAL CRIMES WERE COMMITTED

2. I submit this affidavit for the limited purpose of establishing probable cause in support of a criminal complaint charging DAVID ROSENHOLM with money laundering, conspiracy to commit money laundering, and conspiracy to commit wire fraud, in violation of 18 U.S.C. §§ 1956(a)(3)(A), (B), and (h) and 1349.

3. The facts in this affidavit come from my personal involvement in this investigation, my training and experience, other law enforcement agents, two cooperating witnesses (“CW1” and “CW2”), and other sources identified below. This affidavit does not set forth all of my knowledge about this matter or investigation.

4. Based on the information provided below, there is probable cause to believe that from about August 2018 to at least November 2019, ROSENHOLM and co-conspirators, including, without limitation, Co-Conspirator #1 (CC1), who resides in India, and Co-

Conspirator #2 (CC2) (collectively, the “Target Subjects”), who lives with ROSENHOLM at the Target Location, agreed to launder the proceeds of wire fraud schemes through accounts and businesses controlled by the Target Subjects.

5. The wire fraud scheme involved using purported customer service call centers in India to deceive victims into believing that their computers had been attacked by malware and required remote repair, or that the victims owed money due to an overpaid refund. In furtherance of this scheme, the Target Subjects concealed the origins of money obtained via the computer support and refund fraud scams through banking transfers and commercial transactions, including international and domestic wire transfers. The Target Subjects also schemed to access fraudulently obtained funds controlled by financial institutions by means of false pretenses.

6. In May 2019, the FBI arrested CW1 on charges including wire fraud, bank fraud, telemarketing or email marketing fraud, and conspiracy, in violation of 18 U.S.C. §§ 1343, 1344, 2326, and 1349, all involving similar schemes but different victims and conduct from the victims and conduct discussed herein. CW1 thereafter began cooperating with the government in hopes of receiving a reduced sentence. CW1 has not yet been convicted in that pending matter or convicted of any crimes in the United States. The United States has not entered into a cooperation or a plea agreement with CW1 and has not otherwise made representations to CW1 about the outcome of CW1’s cooperation or the disposition of the pending matter.

7. In an interview pursuant to a proffer agreement and as part of his or her cooperation, CW1 told the FBI that he or she purchases call center data, including victim telephone numbers, to be used to defraud victims based on a number of schemes, including technical computer support and refund scams. CW1 stated that CW1 worked with the Target Subjects and CW2 to defraud victims and arranged for the victim funds to be laundered so that

they could be paid to CW1 and co-conspirators without being thwarted by financial institutions in the United States.

8. In August 2019, the FBI arrested CW2 in the United States on charges including wire fraud, conspiracy to commit wire fraud, and aggravated identity theft, in violation of 18 U.S.C. §§ 1343, 1349, and 1028A, respectively. After CW2's arrest, CW2 also began cooperating with the government in hopes of receiving a reduced sentence if he or she pleads guilty in the pending matter, which concerns a similar scheme but different victims and conduct from the victims and conduct discussed herein. CW2 has not yet been convicted in that pending matter and has not previously been convicted of any crimes in the United States. The government has not entered into a cooperation or a plea agreement with CW2 and has not otherwise made representations to CW2 about the outcome of CW2's cooperation or the disposition of the pending matter.¹

9. In a proffer interview and as part of his or her cooperation, CW2 described himself/herself to the FBI as a middleman who connects money laundering facilitators to call center brokers for a fee. CW2 stated that CW2 acted in a middleman capacity in conspiracies involving CW1 and the Target Subjects, knowing that the laundered funds was money obtained from victims through various criminal fraud schemes. CW2 stated that he/she acted as an intermediary to earn a percentage of the laundered victim funds.

10. CW1 and CW2 have told investigators that, based on their prior involvement with the Target Subjects, they each have direct knowledge of, and participated in, the frauds described

¹CW2 stopped cooperating with the ongoing investigation after an interview on February 27, 2020 in which the government inquired about CW2's involvement in a different scheme.

below that generated the proceeds that have been laundered by the Target Subjects. I have corroborated numerous statement by CW1 and CW2 upon which I have relied in this Affidavit using WhatsApp chats from CW1's and CW2's cell phones and using bank records and information I obtained from victims discussed herein.

The Schemes to Defraud

11. According to CW1 and CW2, one fraud schemes funding the money laundering operation is a computer technical support fraud that is initiated through a pop-up advertisement on a victim's computer. The pop-up advertisement tells the victim that the victim's computer has been attacked by malware and provides a telephone number to call for technical assistance. The pop-up deceives the victim into believing that the advertisement and phone number are associated with a legitimate technical support company, like Microsoft. When the victim calls the number, instead of reaching bona fide technical support, the victim connects to a call center in India where operators offer purported anti-virus or anti-intrusion services in exchange for payment. The victim does not receive the promised services. Indeed, the victim's computer does not require the proffered services. Rather, the operators in the call center merely disable the pop-up advertisement and falsely characterize their actions as virus removal. In exchange for this fake service, the operators obtain money from the victims and direct the victims to send funds into the money laundering network in which both CW1 and CW2 participated.

12. CW1 and CW2 also identified refund scams as another scheme that generate victim funds that must be laundered. In one refund scheme, call centers use email, pop-up advertisements, and telephone calls to notify victims that they are owed a refund from a computer technical support company or from companies like Amazon or PayPal. The victims are told that to receive the refund they must manually enter the dollar amount that they are owed

into an application that is opened for the victims on the victims' computers. During the call, the call center operator gains remote access to the victim's computer and monitors the victim as they input the amount they are told into a screen. When the victim presses enter on the instructed amount, the screen reflects a higher amount than what the victim put in. The intent is to convince the victim that he or she entered a higher amount and that the additional funds must be paid back to the call center. In order to correct the alleged overpayment, the call center operator directs victims to transfer funds from their accounts to an account identified by the call center operator. At times, the call centers also use the scheme to acquire victim funds without the victim's involvement, by taking remote access of the victim's computer or by taking over the victim's financial account online.

The Money Laundering Scheme

13. According to CW1 and to CW2, after victims agree to pay for the fictitious technical support or to send funds as part of a refund scam, the call centers need to disguise the victim funds as legitimate payments to companies with operations in the United States. CW2 reported that middlemen, like him/her, act as a link between call centers and money laundering facilitators who conceal the nature of the victim funds by passing the money through a series of financial transactions. Disguising the funds lessens the likelihood that the victim payments will be stopped or recalled by financial institutions prior to being received by the co-conspirators operating the call centers that initiated the fraud. Each co-conspirator involved in the money laundering scheme, including middlemen and account holders in the United States, provides their services to the money laundering network for a negotiated cut of the fraudulent proceeds.

The Conspirators

14. CW1 and CW2 identified CC1, known only by a WhatsApp² handle (“CC1 Handle”) to CW1, as a money launderer in India, and ROSENHOLM, also known as “Dave,” as a money laundering account holder in the United States. According to CW2, CC1 provides a variety of money laundering services to call centers executing the technical support and refund schemes discussed above, including connecting call centers with account holders in the United States who conduct victim fund transactions using accounts in the United States. CW1 told the FBI that he or she used CC1 to launder money from fraud. Both CC1 and the account holder receive a cut of the proceeds. CW1 and CW2 identified ROSENHOLM as one of the account holders with whom CC1 works to launder victim funds.

15. When the FBI arrested CW1 in May 2019, FBI agents seized his/her four cellphones and, after obtaining consent, searched them. In the cellphones (hereinafter CW1 Cell Phones), agents found the WhatsApp application loaded, operational, and capable of communication with other WhatsApp users as well as other applications like iMessage. CW1 told FBI agents that he/she regularly communicated about the fraudulent activities with co-conspirators, including CW2, using his/her cellphones.

16. When the FBI arrested CW2 in August 2019, agents seized CW2’s cellphones and after obtaining consent, searched them. In one of the cellphones (hereinafter “CW2 Cell #1), agents found the WhatsApp application or software loaded, operational, and capable of communication with other WhatsApp users. CW2 told FBI agents that he/she used CW2 Cell #1

²WhatsApp is a software application that allows smartphone users to communicate with other WhatsApp users through text messaging, telephone calls, and video chats.

to communicate with co-conspirators who execute, among other things, the fraud schemes discussed herein.

17. CW2 told FBI agents that CC1's WhatsApp contact information could be found in the WhatsApp contact list in CW2 Cell #1 under the handle of "CC1 Handle."³ I examined CW2 Cell #1 and found a contact under the CC1 Handle. The WhatsApp profile listed the phone number associated with CC1 Handle as ending 492. The "Business Details" for the CC1 Handle WhatsApp contact shows the category of business as Education. In WhatsApp chat messages between CW2 and CC1 Handle on CW2 Cell #1, CC1 Handle identifies himself as an individual by the name of CC1 with a Skype handle based on CC1's name. In a 2015 publicly available e-commerce chat support group website, an individual using the name of CC1 and the Skype handle referenced above advertised that he could provide technical services through his business.

18. Consistent with CW1 and CW2's assertions regarding CC1's role in the fraud schemes discussed above, CW2 Cell #1 contains WhatsApp chats in which CC1 offers numerous financial services, including bank wires, money transfer services, gift cards, and cash applications. CW2 reported that CC1's offers show the various money laundering services that CC1 can provide to individuals executing various fraud schemes. CC1 states that he can provide services in countries including the United States, United Kingdom, Australia, and Canada.

19. CW2 reported that CW2 met ROSENHOLM through CC1, who told CW2 that ROSENHOLM could provide bank accounts in the United States for laundering call center victim funds. Consistent with CW2's assertions, and as discussed in detail below, WhatsApp

³I know from my use of WhatsApp that the application displays the profile image from the contact's WhatsApp profile, which is generally input by the user or the person who created the user's account with WhatsApp.

chats with CC1 in CW2 Cell #1 show that CC1 used ROSENHOLM as a domestic United States contact who facilitated transfers of victim funds through bank accounts that he controls, either directly or through another individual (CC1).

20. In the WhatsApp chat messages with CW2, CC1 provides the Target Location as ROSENHOLM's address. CC1 also identifies ROSENHOLM as the owner of a First Tech Federal Credit Union ("First Tech") bank account for an entity called "Mongoose Maniacs". Bank records for Mongoose Maniacs contain the same address for ROSENHOLM that CC1 gave to CW2. Using databases available to law enforcement, investigators have also confirmed that the address for the Target Location is associated with David Eugene Rosenholm. A Residential Loan Application shows ROSENHOLM and Co-Conspirator#1 refinancing a home in 2009 with the Target Location listed as the subject property address. Additionally, according to Verizon Wireless records, the phone number associated with the relevant ROSENHOLM bank accounts belongs to ROSENHOLM. Bank camera photographs of an individual conducting transactions through the Mongoose Maniacs' account at First Tech show a person who also appears pictured on ROSENHOLM's Oregon state driver's license, which I have reviewed.

21. CC2 as discussed below, is a co-signor on several corporate accounts with ROSENHOLM; she is also an individual signor on an account used to launder money for call center fraud. CC2 is an officer of Mongoose Maniacs. In databases available to law enforcement, CC2's address is the same as ROSENHOLM's. CC2's driver's license, social security number, and date birth all appear to have been used to open the below-referenced bank accounts that ROSENHOLM shares. Bank camera photographs of an individual conducting transactions through the corporations discussed herein show a person who also appears pictured

on CC2's Oregon state driver's license. Bank records list CC2's email that investigators have identified based on Google subscriber records.

The Manner and Means of the Money Laundering Conspiracy

22. ROSENHOLM and CC2 have created and jointly used bank accounts and at least two corporations, Mongoose Maniacs, Inc. ("Mongoose Maniacs") and Kre8change Beaverton ORE LLC ("Kre8change"), and other associated bank accounts to receive and to disburse the proceeds of the fraud schemes discussed above.

23. ROSENHOLM and CC2 have had interconnected banking relationships since at least 1998:

a. In May 1998, CC2 opened a joint bank account at First Tech Federal Credit Union with ROSENHOLM.

b. On February 3, 2018, ROSENHOLM opened an individually owned checking account at Bank of America (the "ROSENHOLM BOA Account").

c. On July 26, 2018, ROSENHOLM opened a checking account in his name at Wells Fargo Bank, N.A. (the "Rosenholm Wells Fargo Account"). On the application, ROSENHOLM listed his employer as Mongoose Maniacs, Inc.

24. Mongoose Maniacs is a Wyoming corporation created June 14, 2011. The company's 2012 Annual Report lists ROSENHOLM as the director and only officer of the corporation. The contact email on Mongoose Maniacs' corporate filings is dave.rosenholm@gmail.com, and the contact telephone number also belongs to ROSENHOLM. Other than in 2013, when MVI Corp.⁴ is listed as an officer of Mongoose Maniacs, corporate

⁴ MVI is a corporation created by WyomingRegisteredAgent.com, which has registered hundreds of corporations.

documents identify ROSENHOLM as its director from 2012 to 2019. In 2015, CC2 was identified as the treasurer/fiscal agent and as the vice president in 2016 and 2019. On June 17, 2011, ROSENHOLM opened an account for Mongoose Maniacs at Bank of America (“Mongoose BOA Account 2365”). The account opening documents identify ROSENHOLM as the President of the corporation and CC2 as the secretary. That same day ROSENHOLM and CC2 opened another Mongoose checking account (“Mongoose BOA 2352”). On or about February 7, 2018, ROSENHOLM opened a savings account for the benefit of Mongoose Maniacs, Inc. (“Mongoose BOA Account 3361”).

25. ROSENHOLM and CC2 opened a checking account or Mongoose Maniacs at Wells Fargo on or about February 2, 2018, , and a savings account on or about June 17, 2011. The bank account opening documents identify ROSENHOLM and CC2 as co-signers. ROSENHOLM is listed as the owner of the Mongoose Maniacs and CC2 as responsible for “Marketing.” Bank records list ROSENHOLM’s phone number as the contact for the corporation, the Target Location as the mailing address, and state that the corporation provides marketing services.

26. On or about May 14, 2019, ROSENHOLM and CC2 opened an account for Mongoose Maniacs at First Tech Federal Credit Union (“Mongoose First Tech Account”). Bank records list ROSENHOLM and CC2 as the sole signatories and identify ROSENHOLM the President and CC2 as the vice president. The listed account owner address in the Business Account Application is the Target Location. ROSENHOLM’s cellphone number is listed as the business phone number associated with the Mongoose First Tech Account. The stated purpose of Mongoose Maniacs in the First Tech account opening documents is “Direct sale of Frontier Communications TV, internet phone sale Fios.” CC2 is listed in the account opening documents

as the individual “with significant responsibility for managing” the corporation and vice president.

27. Kre8change is an Oregon corporation created by ROSENHOLM on February 27, 2018. The Kre8change incorporation documents list ROSENHOLM as the sole authorized agent, organizer, and individual with direct knowledge. Kre8change’s 2019 Amended Annual Report states that Kre8change is a business that provides “humanitarian assistance to humanity.” ROSENHOLM is also listed in the 2019 documentation as the registered agent, manager, and president of the corporation.

28. On or about March 1, 2018, ROSENHOLM opened an account for Kre8change at U.S. Bank (“Kre8change U.S. Bank Account”). The bank opening documents list ROSENHOLM as the sole authorized agent and member of Kre8change and lists the Target Location as the business address. According to a U.S. Bank employee, the Kre8change U.S. Bank Account documents reflect ROSENHOLM’s profession as “homemaker.”

29. On or about March 5, 2018, ROSENHOLM opened checking account at Bank of America for the benefit of Kre8change Beaverton ORE LLC (“Kre8change BOA Account”). ROSENHOLM listed himself as the sole authorized signor and member, and provided the Target Location on the account opening deposit slip.

30. Mongoose Maniacs and Kre8change appear to exist only on paper; neither has a physical office space or any apparent employees; neither appears to provide any actual services or to sell any products to bona fide customers. Both were created with minimal supporting documentation and have minimal online presences. Based on my training and experience, I believe that Mongoose Maniacs and Kre8change are “shell” corporations that are being used as fronts for criminal activity, including money laundering. As discussed below, ROSENHOLM

and CC2 used the corporations to obscure their identities and to create an appearance of legitimacy for financial transactions that concealed the fraudulent nature of the transactions from the victims of the fraud schemes discussed above.

Acts in Furtherance of the Fraud and Money Laundering Conspiracies

31. Victim #1, whom I have interviewed, is a resident of California. On or about August 2018, Victim #1 received a phone call from someone asserting they were with PC Booster, a company that Victim #1 had previously paid \$399 for technical support services for her computers. The purported PC Boosters representative told Victim #1 the company was having licensing issues and could no longer provide the services that they had contracted for. Thus, the company was refunding \$150 to Victim #1. To receive the refund, Victim #1 gave the caller remote access to her computer and input the number 150 into an application that the caller brought up on her computer screen. When Victim #1 input \$150, however, the application displayed \$15,000 instead. Victim #1 stated that, at that point, the caller became angry with Victim #1 and told her that her mistake resulted in a \$15,000 transfer into her account instead of \$150. To rectify the error, the caller told Victim #1 that she needed to access her bank account and wire the surplus money to different individuals associated with the company. Victim #1 stated that, unbeknownst to her, although her account reflected a surplus, the increased balance was due to an unauthorized transfer of funds from her savings account to her checking account. Financial records show that on or about August 6, 2018, Victim #1 wired \$7,000 from her checking account to ROSENHOLM's Wells Fargo Account. Financial records also show that on August 9, 2018, ROSENHOLM wired \$6,250 to CC1.

32. Victim #2, whom I have interviewed, is a resident of Florida. On or about August 2018, Victim #2 received a call from an unknown individual claiming to be with a computer

service company. The caller told Victim #2 that she was owed a \$500 refund for a computer related security program that she purchased. The caller thereafter gained remote access to Victim #2's computer and bank account. Victim #2 reported that she was then told that when the caller attempted to refund her money, a mistake was made. According to the caller, while processing the \$500 refund, \$5,000 had been mistakenly put into Victim #2's bank account. Victim #2 reported that she was told that in order to return the \$4,500 overpayment, the caller needed to access Victim #2's bank account. Financial documents show that after the call, Victim #2's bank account was accessed, and, on or about August 13, 2018, \$4,400 was wired from Victim #2's Bank of America account to the Kre8change U.S. Bank Account. Contrary to the caller's assertions, Victim #2 stated she was not paid \$5,000 by a computer service company in August 2018. Rather, Victim #2 said the \$4,400 wire came out of Victim #2's own funds.

33. Victim #2 stated that she had no business dealings with a company called Kre8change nor with its owner, ROSENHOLM. Financial records reflect that after receiving the \$4,400 and other deposits, ROSENHOLM wired \$4,802 to CC1 on August 14, 2019.

34. Victim #3, whom I have interviewed, is a resident of California. In early 2019, Victim #3's computer was beeping and malfunctioning. Around the same time, Victim #3 received an email purportedly from Microsoft alerting her that her bank account had been hacked. Victim #3 called the number provided in the email and spoke with someone who identified himself as "Joseph." Joseph communicated to Victim #3 that she was owed \$330. Victim #3 stated that Joseph told her to enter \$330 into an application on her computer. When Victim #3 entered the amount, she was told by Joseph that she had mistakenly entered \$30,000. Victim #3 stated that she was told that, due to her error, she'd received \$30,000 into her account and needed to rectify the overpayment. Victim #3 was also told that she owed other funds to the

call center for investments and for other reasons described to her by the call center caller. Victim #3 stated that at Joseph's direction, Victim #3 wired, among other amounts, \$45,000 to the Kre8change U.S. Bank Account on February 2, 2019. On or about February 5, 2019, CW2 sent CW1 an image of Kre8Change's U.S. Bank Account statement reflecting the \$45,000 deposit from Victim #3. Financial documents show that after receiving the funds, on or about February 5, 2019, ROSENHOLM initiated a \$30,020 wire to CW1. CW1 reported that he/she received the funds because of a business relationship he/she had with the call center that spoke with Victim #3 and caused her to send the wire. On or about the same day, February 5, 2019, ROSENHOLM wired \$8,065 to CC1 from the Kre8change U.S. Bank Account. Financial records show that in February 2019, U.S. Bank was notified by First Bank of Tennessee, another victim's bank, that the Kre8change U.S. Bank Account had received fraudulent funds. U.S. Bank called Victim #3 to discuss Victim #3's wire as it occurred close in time to the reported fraudulent wire. Victim #3 gave the U.S. bank employee an explanation for the wire that was inconsistent with ROSENHOLM's explanation and the employee ultimately determined that the wire had been sent under fraudulent pretenses and, thus, U.S. Bank requested debit authority from ROSENHOLM for the return of Victim #3 funds. ROSENHOLM gave debit authority, and on or about February 13, 2019, \$45,000 was debited from the Kre8chnage U.S. Bank Account and wired to Victim #3.

35. Victim #4, whom I have interviewed, is a resident of Tennessee. Prior to February 2019, Victim #4 received a pop-up message on his computer that appeared to be from Microsoft. The pop-up alerted Victim #4 that his computer was infected with a virus, which needed to be fixed if he wanted his computer to be operational. Accompanying the pop-up was a toll free number, which Victim #4 called for computer services. The individual with whom

Victim #4 spoke offered to provide computer services for a fee, which Victim #4 paid. At some point thereafter, the computer service provider called Victim #4 back and told him that the computer service company owed him a refund because he had overpaid. Rather than receive a refund, however, Victim #4's bank notified him that \$18,000 had been wired on or about February 5, 2019 from his account to the Kre8change U.S. Bank Account. Victim #4 stated that the \$18,000 wire was sent without his knowledge or authorization. Financial records show the day following the \$18,000 wire, ROSENHOLM spent \$1,999 at Best Buy, withdrew \$1,000 cash, wrote a \$12,195 check to CW1, and wired \$2,115 to CC1 from the Kre8change U.S. Bank Account. CW1 has told the FBI that the purpose of this payment from ROSENHOLM was to compensate the parties involved for their roles in defrauding the victim and moving the funds at issue. Financial records show that after the wires and check issued by ROSENHOLM, a First Bank employee notified U.S. Bank that the Kre8change U.S. Bank Account received Victim #4's funds because of fraud. Victim #4's financial institution requested a recall of the funds. ROSENHOLM spoke with a representative of U.S. Bank on or about February 6, 2019 regarding Victim #4 transaction. The call was apparently recorded by ROSENHOLM, and ROSENHOLM provided the call recording to CC1 who sent it to CW2, who then provided it to CW1 over WhatsApp. In the recording, ROSENHOLM contended that the funds sent by Victim #4 were part of "a legit wire" and that he would not be "returning the funds." ROSENHOLM stated that he builds aquaponics units and that the funds at issue were intended for aquaponics products for "greenhouses and stuff like that." ROSENHOLM stated that he gets the equipment for customers generally and intended to get the equipment to Victim #4 after he received the funds for their purchase. Financial records show that, consistent with a request to return the funds to

Victim #4 based on fraud, on February 8, 2019, \$18,000 was debited from the Kre8chnage U.S. Bank Account and wired to Victim #4.

36. Victim #5 is a resident of Oregon. Sometime before February 2019, Victim #5 received a popup message on his computer screen stating there was an error with his computer. The message provided a phone number to call; Victim #5 believed the popup and called the number. Subsequently, Victim #5 received a call purportedly from a computer support company. The caller told Victim #5 that the company wanted to refund him \$500 because the tech support company was no longer supporting Microsoft products and could not provide all the services that Victim #5 had contracted for. Victim #5 gave the purported technical support caller remote access to his computer and they brought up a screen for him to input the refund amount. After Victim #5 entered in \$500, the individual with whom Victim #5 spoke told Victim #5 that he had put \$50,000 into the program instead and became irate. The caller told Victim #5 that the overpayment would need to be returned by Victim #5 to correct the error.

37. CW1 was associated with the call center that contacted Victim #5, caused him to give remote access to his computer, and convinced him that he had been overpaid for a refund. After a co-conspirator known to CW1 obtained access to Victim #5's funds, CW1 contacted CW2 to arrange for movement of Victim #5's funds through an account in the United States. Thereafter, CW2 arranged with CC1 to move Victim #5's funds through ROSENHOLM's Kre8change U.S. Bank account to other accounts identified by CW1 for payment.

38. Financial documents show that after the calls from the purported computer support employee, on or about February 4, 2019, \$50,000 was transferred from Victim #5's savings account to his checking account without his knowledge or consent. Similarly, financial records show that on or about February 6, 2019, \$100,000 was transferred from Victim #5's

savings account to his checking account without his knowledge or consent. Both the \$50,000 and \$100,000 were part of a \$287,834.32 deposit into Victim #5's account in September 2018 from the sale of his home. A caller from the purported computer support company told Victim #5 that the \$50,000 transfer and \$100,000 transfer came, not from his own account but, rather, from the computer support company. Victim #5 stated that the caller told him that he could keep \$1,500 of the money because of the inconvenience, but that the remainder would need to be wired to the computer support company. Financial records show that on or about February 6, 2019, \$98,500 was wired from Victim #5's account to the Kre8change U.S. Bank Account. Victim #5 stated that he was questioned about the transfer by his financial institution, but he did not respond because, based on what the purported computer support caller told him, he believed that the funds did not belong to him.

39. On or about February 6, 2019, a U.S. Bank employee contacted ROSENHOLM about the fraudulent wires received from Victim #3, Victim #4, and Victim #5. According to the U.S. bank employee, ROSENHOLM was evasive and stated that he was in the business of being a humanitarian for humans. ROSENHOLM told the analyst that he sold unspecified products and otherwise gave money away. When the U.S. bank employee told him that Victim #4 wired money into his account because of a tech scam, ROSENHOLM authorized the funds to be returned to both Victim #4 and Victim #3. As noted above, on or about February 8 and February 13, 2019, U.S. Bank withdrew \$63,000 from the Kre8change U.S. Bank Account to return funds to Victim #4 and Victim #3.

40. CW1 Cell #1 contains a series of WhatsApp conversations involving CW1, CW2, CHOWDURY, and ROSENHOLM regarding Victim #5 wire into ROSENHOLM's account. Specifically, WhatsApp chats show that after the complaints of fraud by Victim #4, CC1 told

CW2 that Victim #5's funds were frozen in ROSENHOLM's Kre8change U.S. Bank Account. For example, ROSENHOLM wrote via WhatsApp, "Because the 18 k fucker then the 45 k fucker claimed fraud they automatically thin[k] [Victim #5] wire a fraud." CW2 told CW1 via WhatsApp chats that after the funds were frozen, ROSENHOLM went to U.S. Bank and tried to convince the bank that the frozen funds were part of a legitimate transfer for a hydroponics business deal. CW2 forwarded jpg images of messages between ROSENHOLM and CC1 wherein the two discuss the steps that ROSENHOLM had taken to get the funds released and what the other co-conspirators could do to help:

Series #1

Date	Time	Sender	Receiver	Message
Unkn ⁵	3:58	ROSENHOLM	CC1	Ok the bank will investigate then once done they will release funds
Unkn	3:59	CC1	ROSENHOLM	Okay did they mention any tym frame So that according I can hold this client for further payments ?
Unkn	4:00	ROSENHOLM	CC1	Maybe 1 day
Unkn	4:01	CC1	ROSENHOLM	Okay kool let me hold this till tomorrow post this one then
Unkn	4:02	CC1	ROSENHOLM	We will do futhera
Unkn	4:20	ROSENHOLM	CC1	Ok
Unkn	4:23	CC1	ROSENHOLM	We got a total of 150k more held it till tomorrow hoping for the best and from now on gonna say its for aquapontiacs
Unkn	4:32	ROSENHOLM	CC1	Yes

⁵ Screenshots of the messages between CC1 and ROSENHOLM were sent from CW2 to CW1 on February 8, 2019.

Unkn + 1	3:24	CC1	ROSENHOLM	Dave did you get any call from the bank or any update
Unkn + 1	4:53	ROSENHOLM	CC1	I just called the lady Rachel at the bank. She said tops 7 working days

Series #2

Date	Time	Sender	Receiver	Message
Unkn ⁶	3:00	ROSENHOLM	CC1	He Russell simply needs to verify he authorized funds to be wired to kre8change with his permission
	3:01	ROSENHOLM	CC1	For business purposes for Aquaponics
	3:01	CC1	ROSENHOLM	Yes on it still
	3:01	ROSENHOLM	CC1	Simple

Series #3

Date	Time	Sender	Receiver	Message
Unkn ⁷	21:48	ROSENHOLM	CC1	I just spoke with [U.S. Bank employee] at US Bank in ohio. She said Russell has not contacted her also his bank has not validated the wire transfer payment. So with that being said Russell needs to call [U.S. Bank employee] @ Us bank 1-513-[XXX-XXXX]. Simply verify that the funds were sent intentionally to Kre8change for business purposes that we are doing
Unkn + 1	1:12	CC1	ROSENHOLM	Sorry I missed ur call but i seriously have no clue cz the

⁶An image of the messages between CC1 and ROSENHOLM was forwarded from CW2 to CW1 via WhatsApp on 2/19/19.

⁷*Id.*

				recordings sent shows Russell has called the banker and spoken lemme again ping them
Unkn + 1	1:13	ROSENHOLM	CC1	In recording I never hear the lady only him
Unkn + 1	1:14	ROSENHOLM	CC1	This needs done today please

41. As shown in the WhatsApp text messages above and in WhatsApp voicemail messages from CC1, CC1 communicated to CW2 in February 2019 that ROSENHOLM's attempts to unfreeze the funds himself were unsuccessful and that, in order for the funds to be released, Victim #3 needed to say the funds were sent for "aquapontiacs construction." On or about February 20, 2019, CW2 communicated to CW1, in substance, that he/she needed to find someone who could call the bank, posing as Victim #5, and get the funds released.⁸ CW2 told CW1 that ROSENHOLM would create a video of himself showing that he was locked out of his account. Later that same day, CW1 sent a video of an individual, whom I believe to be ROSENHOLM, attempting to log into the Kre8Change U.S. Bank Account from what appears to be a home computer with the username Kre8change1Beaverton. When the individual entered a password, the screen displayed, "Sorry our system is currently unavailable. Please try again." The male voice in the video stated that the "Please try again" message meant his "fucking account's locked" and he "can't get in." To have the Kre8change account unlocked, the male requested that the viewer(s) of the video have Victim #5 call and say that the \$98,500 wire was sent from him to the Kre8change account.

⁸My understanding of the February 20, 2019 conversation comes from a recorded Hindi phone conversation in CW1 Cell #1, of which an FBI-certified linguist created a draft translation.

42. On or about February 20, 2019, an unidentified individual who uses the WhatsApp handle “XYZ” (“CC3”), called U.S. Bank from a U.S. number posing as Victim #5, in an attempt to have the funds released. During the call, CC3 told the U.S. Bank employee that he wanted his funds released to ROSENHOLM, and that the funds were sent to ROSENHOLM for a greenhouse construction business project.

43. I have spoken with Victim #5 and listened to recordings of his voice on calls with First Tech employees. I have also listened to the February 21, 2019 recorded conversation with the U.S. Bank employee. The speaker on the February 21, 2019 recorded call is a male who has an accent and voice different from Victim #5.

44. Notwithstanding ROSENHOLM’s and CC3’s attempts to convince U.S. Bank that the transactions in the Kre8change U.S. Bank Account were legitimate, U.S. Bank closed ROSENHOLM’s account on or about February 21, 2019 due to fraudulent activity and issued the remaining balance in the account, \$55,721.10 to ROSENHOLM.

45. According to bank records, on or about that same date, ROSENHOLM and CC2 went to a First Tech branch to open a new business account. According to a First Tech employee, ROSENHOLM stated that he had an account at U.S. Bank, but that U.S. Bank made him mad and, thus, he needed a new account. ROSENHOLM told the First Tech bank employee that he expected to receive “hundreds of thousands of dollars” each month from Africa and India to fund his new hydroponics business growing vegetables. He stated that customers would pay him for his technology. ROSENHOLM told the First Tech employee that although he had other businesses, he did not make money from them.

46. According to bank records, when a First Tech employee did a background check on ROSENHOLM, she found that ROSENHOLM had a Chexsystems freeze.⁹ ROSENHOLM told the First Tech employee that the freeze resulted from an interaction between a customer and another of his businesses to which the customer paid “a couple hundred thousand dollars” but then recalled. ROSENHOLM told the First Tech employee that he did not use the disputed money and that Bank of America contended he received the funds at issue because of fraud. The First Tech employee noted that CC2 was sitting next to ROSENHOLM holding a cashier’s check from U.S. Bank that ROSENHOLM wanted to deposit into a First Tech account. ROSENHOLM stated that he wanted to deposit the check so that he could buy silver. According to the First Tech employee, ROSENHOLM and CC2 could not open a new business account in February 2019 at First Tech because of the ChexSystems freeze.

47. Bank records show that on or about February 21, 2019, CC2 deposited the \$55,721 check into CC2’s personal First Tech account. From the \$55,721 deposit, CC2 wired \$11,226.80 to CC1 on or about February 25, 2019. CC2 also withdrew several thousand dollars and spent several thousand more on personal expenses over a two-month period. Review of case evidence has not identified any expenditures on hydroponic equipment, supplies, or services by ROSENHOLM or CC2.

48. Victim #6, whom I have interviewed, is a resident of Florida. On or about November 14, 2019, an individual purporting to be from Amazon called Victim #6 and informed her that her husband’s Amazon account had a credit of approximately \$300. The caller directed

⁹ A Chexsystems freeze is a security freeze on an individual’s ability to conduct financial transactions designed to prevent credit, loans and services from being approved in an individual’s name without their consent.

Victim #6 to go to her computer to access the refund. After Victim #6 accessed her computer for purposes of the refund, a pop-up advertisement appeared on the screen. Victim #6 stated that she may have given the caller remote access to her computer for purposes of receiving the Amazon refund. Victim #6 reported that despite the caller's representations, Victim #6 did not receive a credit from Amazon into her bank account. Rather, on or about November 15, 2019, an unauthorized individual initiated two wires totaling \$85,572.86 from Victim #6's bank account into the Mongoose First Tech savings account. Following the deposit into the Mongoose First Tech savings account, the funds were transferred to the First Tech Mongoose Checking account.

49. Financial records show that following the wires into the Mongoose First Tech Checking Account, several personal expenses were paid out of the account and \$2,500 was withdrawn. ROSENHOLM and CC2 are the only signers on the account at issue. On or about November 25, 2019, ROSENHOLM, with a transaction note stating "from Dave," wired \$72,686 to CC1. The stated purpose of the wire to CC1 was "repayment of loan." Financial records show that on or about December 6, 2019, an employee of First Tech called ROSENHOLM about the transactions involving Victim #6. ROSENHOLM told the employee that he never had direct contact with Victim #6 regarding the wire, but that he understood the funds from Victim #6 were part of a hydroponics business transaction. The First Tech employee asked why Victim #6 would buy hydroponics when the account opening documents stated that Mongoose Maniacs was an internet company, but ROSENHOLM did not explain.

50. According to the Sheriff's Office for St. Lucie County, Florida, on or about November 16, 2019, Victim #6 reported that she was the victim of fraud. On or about April 3, 2020, a St. Lucie County Sheriff's Office detective spoke with ROSENHOLM to discuss the \$85,572.86 wired into the Mongoose First Tech Account. During the call, ROSENHOLM

identified himself as the joint owner of the Mongoose account and stated he had been the owner of Mongoose Maniacs business “off and on.” ROSENHOLM stated that the company did “humanitarian things,” and that he was involved in internet sales and aquaponics.

ROSENHOLM told the detective that he has resided at the Target Location for about 20 years.

51. ROSENHOLM told the detective that he was familiar with CC1. Specifically, ROSENHOLM stated that CC1 is a “leads” broker for him and is known to him now to be a scammer. ROSENHOLM stated that the \$72,686 sent to CC1 was for the purchase of supplies. ROSENHOLM stated that sometimes it takes months to get supplies from CC1 and that he had yet to receive the supplies he purchased for Victim #6’s benefit. ROSENHOLM stated that he would go to the police department and file a complaint regarding the concerns that the detective revealed about his account and Victim #6’s funds.

Intent to Defraud and Knowledge of that Specified Unlawful Activity

52. In October 2019, acting at the direction of FBI agents, CW2 sent series of WhatsApp messages from Massachusetts to CC1. Specifically, on October 30, 2019, CW2 contacted CC1 using WhatsApp and asked him to identify an account through which victim funds from a tech support services fraud could be laundered. CW2 messaged, “I have a fake physical wire for 5000\$ today give me good % I will do it ryt [sic] away. Its for tech support call centre.” CW2 told the FBI that based on his/her experience with CC1, the verbiage, “fake physical wire” and “for tech support call centre [sic],” specified that the money being directed to the bank account was the proceeds of tech support call center fraud. In response to CW2’s inquiry, on October 31, 2019, CC1 messaged:

Date	Time	Sender	Receiver	Message
11/1/2019	11:13	CW2	CC1	I have a fake physical wire for 5000\$ today give me good % I will do it ryt away

11/1/2019	11:13	CW2	CC1	It's for tech support call centre
11/1/2019	11:14	CC1	CW2	Baba for physical wire and amt 5 K Usd Payout will be 65% Dollar rate Rs. 65
11/1/2019	11:15	CC1	CW2	But amt make sue its either 4986 or 5124 or so whatever like that
11/1/2019	11:15	CC1	CW2	Not even amt
11/1/2019	11:16	CC1	CW2	Sure no issue matlab charge back bhi ho sakta hai
11/1/2019	11:17	CC1	CW2	Make sure its done before 12 pm usa banking hrs to aaj hi withdraw bhi honayega

Based on the context of the conversation, information provided by CW2, and my training and experience, I understood CC1 to say that he agreed to launder \$5,000 for a 35% cut of the victim funds. The remaining 65% would be wired to CW2 to take his/her cut and to disburse to the call center. Additionally, from CW2 and information regarding the scheme, I understood that CC1 asked that the funds transferred reflect an uneven amount to reduce the likelihood that the transfer would be flagged as fraudulent.

53. Before agreeing to the 35% cut for CC1, CW2, communicating in English, attempted to negotiate CC1 down to a 30% cut of the victim proceeds. CC1 responded, “Baba I am earning a 5% so pls giving u best rate and payment option for amt as 5kusd. Volme yada hoga to percentage bhi reduced milega bhai don't worry.” Based on a translation of the Hindi and the context of the conversation, CW2 indicated that CC1 was stating he would not reduce his rate to 30% for a laundered amount of \$5,000, but that if the volume of deals between CW2 and CC1 increased, he would agree to reduce his cut of the victim proceeds in future transactions.

54. After CW2 told CC1 that the call center would give CC1 a 35% cut of the victim funds, CC1 messaged instructions through WhatsApp detailing how he wanted the transfer conducted and what steps CW2 should take to confirm the wire. Specifically, CC1 wrote:

Date	Time	Sender	Receiver	Message
11/1/2019	11:29	CC1	CW2	But need proper physical wire paper work and also make sure the cust is on hold for min 24 working hrs from the tym of making the transfer
11/1/2019	11:30	CW2	CC1	Which Ac you want me to do the wire and also you will pay my cut today in USA AC once its done
11/1/2019		CC1	CW2	Can be done
11/1/2019		CC1	CW2	Ur cut will be cash deposit in the usa given acct then
11/1/2019		CC1	CW2	And rest payput will be done tomorrow before or on shift tymings

55. CC1 then told CW2 that the funds would be moved through ROSENHOLM and his Mongoose First Tech Account. Specifically, CHOWHURY stated the following via WhatsApp on November 1, 2019:

Date	Time	Sender	Receiver	Message
11/1/2019	11:38	CC1	CW2	And acct to be used is
11/1/2019	11:39	CC1	CW2	David Rosenholm [Target Location] This
11/1/2019	11:39	CC1	CW2	Name of Bank: First Tech Credit union Addr: Cedar, Hills Blvd, Beaverton Oregon, 97005 Name on Account :: Mongoose Maniacs Inc. Number. # [xxxxxx]8650 Routing number

				321180379
				This is the info

CW2 provided CC1 account information for purported call center account (“Fraud Account A”), which was a covert FBI-controlled account.

56. An FBI Undercover Employee (“UCE”) opened Victim Account A at Rockland Trust Bank in Massachusetts. On or about November 4, 2019, the UCE wired \$5,049 from Victim Account A at a Rockland Trust Bank location to the Mongoose First Tech Savings Account identified by CC1. After the wire, the funds were transferred into the Mongoose First Tech Checking Account. Financial records show that, consistent with the payment method for the call center identified by CW2, on November 6, 2019, ROSENHOLM wired \$2,952 of the \$5,049 he received from Victim Account A to Fraud Account A (the FBI-controlled account) that, as noted above, CW2 provided to CC1. Financial records also show that ROSENHOLM also wired \$1,257 to CC1 at a Kotak Mahindra Bank Limited account in India. Wire detail records show that the wire was sent from “David Rosenholm” residing at the Target Location.

57. Bank records show that after the wires to Fraud Account A and CC1, ROSENHOLM and CC2 kept the remaining wired funds in the Mongoose First Tech Checking Account. The amount kept by ROSENHOLM and CC2 plus the wire funds sent to CC1, equate to approximately 40% of the total victim funds. According to the wire detail transfer from ROSENHOLM to CC1, the wire’s purpose was to “purchase supplies.”


58. On or about April 3, 2020, ROSENHOLM was questioned regarding the above-referenced transaction by the St. Lucie County Sheriff’s Department. During the call, the St. Lucie Detective asked ROSENHOLM about the \$2,952 wire he initiated into Fraud Account A. ROSENHOLM said he had “never heard” of the corporation that owned Fraud Account A.

ROSENHOLM stated, however, that the source of the funds was likely a client of CC1's who was referred to ROSENHOLM for "doing some stuff."

CONCLUSION

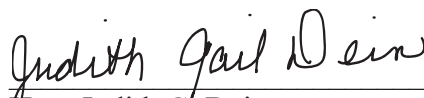
59. Based on the foregoing, I submit there is probable cause to believe that ROSENHOLM committed the following federal crimes:

- a. Conspiracy to commit money laundering to promote wire fraud and to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of the wire fraud, in violation of 18 U.S.C. § 1956(h);
- b. Money laundering, in violation of 18 U.S.C. § 1956(a)(3)(A) and (B), on or about November 6, 2019; and
- c. Conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349.



Vivian M. Barrios
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to by telephone in accordance with Federal Rule of Criminal Procedure 4.1 this 17th day of August, 2020.



Hon. Judith G. Dein
United States Magistrate Judge
District of Massachusetts